SonicWALL Mobile Connect

Mobile Connect for Android 3.1 User Guide

SONICWALL®

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your system.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2014 – 07 P/N 232-002603-00 Rev. A

Table of Contents

Using Mobile Connect for Android

SonicWALL Mobile Connect for Android™ is an **app** that enables Android devices to establish secure, mobile connections to private networks protected by Dell SonicWALL security appliances.

How Mobile Connect Works

Modern business practices increasingly require that users be able to access any network resource (files, internal websites, etc.), anytime, anywhere. At the same time, ensuring the security of these resources is a constant struggle. While most users are aware that they must take care to protect computers from network security risks, this security awareness does not always extend to mobile devices. And yet, mobile devices are increasingly subject to security attacks. Furthermore, mobile devices often use insecure, untrusted, public Wi-Fi hotspots to connect to the Internet. It is therefore a challenge to provide secure, mobile access while still guarding against the inherent security risks of using mobile devices.

The SonicWALL Mobile Connect app for Android devices provides secure, mobile access to sensitive network resources. Mobile Connect establishes a Secure Socket Layer Virtual Private Network (SSL VPN) connection to private networks that are protected by Dell SonicWALL security appliances. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

To get started with SonicWALL Mobile Connect:

1. Install SonicWALL Mobile Connect from the Google Play Store or the Amazon Appstore.
2. Enter connection information (server name, username, password, etc.).
3. Initiate a connection to the network.
4. Mobile Connect establishes a SSL VPN tunnel to the Dell SonicWALL security appliance.
5. You can now access resources on the private network. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

Prerequisites

The following sections describe prerequisites for SonicWALL Mobile Connect:

- Android Product Support on page 5
- Dell SonicWALL Appliance Support on page 5
- Required Network Information on page 6

Android Product Support

SonicWALL Mobile Connect requires the Android 4.0 or newer platform and a cellular or Wi-Fi connection.

SonicWALL Mobile Connect has been verified to run on the following Android devices running the official Android 4.0 platform:

- Dell Venue 7 and 8
- Samsung Nexus 10
- Samsung Galaxy S2
- Samsung Galaxy S3
- Samsung Galaxy S4
- Samsung Galaxy S5
- Samsung Galaxy Tab
- ASUS Nexus 7
- ASUS FonePad
- LG Nexus 4
- LG Nexus 5
- Motorola Droid Razr Tablet
- Amazon Kindle Fire HDX

Note: Although Mobile Connect is designed to work with all Android devices running the 4.0 or newer platform, only the above platforms have been tested and verified to run Mobile Connect. Custom ROMs are not officially supported.

Dell SonicWALL Appliance Support

SonicWALL Mobile Connect is a free app, but requires a concurrent user license on one of the following Dell SonicWALL solutions in order to function properly:

- Dell SonicWALL firewall appliances including the TZ, NSA, E-Class NSA running SonicOS 5.8.1.0 or higher
- Dell SonicWALL SRA appliances running 5.5 or higher
- Dell SonicWALL Aventail E-Class SRA appliances running 10.5.4 or higher

What's New in This Release?

Application Access Control – Support for the Application Access Control feature in Dell Secure Mobile Access 11.0 on E-Class SRA appliances is added in Mobile Connect 3.1. Application Access Control allows remote access administrators to control exactly which resources on the corporate network each application (app) can access. Meanwhile, the device owner can still use their personal Android device for their own activities such as personal email, financial data, pictures, music, accessing third party web sites, etc.

For more information, see Application Access Control on page 29.

Personal Device Authorization – Mobile Connect 3.1 supports the Personal Device Authorization feature in Dell Secure Mobile Access 11.0 on E-Class SRA appliances.

Administrators can configure the E-Class SRA appliance so that users who log in with personal devices are allowed access to the network, provided that the user authorizes the device.

Personal Device Authorization is configured independently of Application Access Control and the two features are not required to be simultaneously enabled.

During the authorization process of the personal device:

- An authorization record is created that associates the device with the user.

- The user must agree to comply with corporate policies regarding access of company data and resources from their personal device.
- The company discloses any privacy ramifications to the user, such as that data from their personal device may be sent to the corporation.

Required Network Information

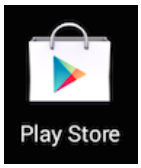
In order to use SonicWALL Mobile Connect, you will need the following information from your network administrator or IT support:

- Server name or address – This is either the IP address or URL of the SSL VPN server that you will connect to.
- Username and password – Typically, you will be required to enter your username and password, although some connections may not require this.
- Domain name – The domain name of the SSL VPN server. Mobile Connect may be able to automatically determine this when it first contacts the server, or there may be multiple domains that can be selected.

Installing Mobile Connect

SonicWALL Mobile Connect is installed through the Google Play Store or the Amazon Appstore.

1. On your Android device, tap the Google Play icon:

   Or, type the following in the browser:

   Google Play Store:
   https://play.google.com/store/apps/details?id=com.sonicwall.mobileconnect

   Amazon Appstore:
   https://www.amazon.com/gp/mas/dl/android?p=com.sonicwall.mobileconnect
2. Go to the **Search** tab, type **SonicWALL Mobile Connect**, and tap **Search**.
3. In the search results, select **SonicWALL Mobile Connect**.
4. Click the **Install** button under **SonicWALL Mobile Connect**. The app will install on your device. When installation is complete, the SonicWALL Mobile Connect icon will appear on your device.

If you encounter an error when attempting to download SonicWALL Mobile Connect, please go to the appropriate site for help:

Google Play Store Help - Follow troubleshooting procedures and instructions on how to report the issue using your Google account: http://support.google.com/googleplay/?hl=en

Amazon Appstore Help - Follow troubleshooting procedures and instructions on how to report the issue using your Google account:
http://www.amazon.com/gp/help/customer/display.html?nodeid=201111910

Using Mobile Connect

The following sections describe how to use Mobile Connect:

Creating a Connection

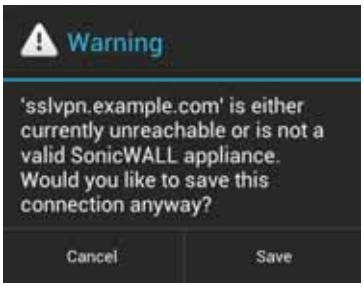
The process of creating a Mobile Connect connection is slightly different depending on which type of Dell SonicWALL appliance you are connecting to. The following sections describe how to create a connection:

Creating a Connection to Dell SonicWALL Firewall and SRA Appliances

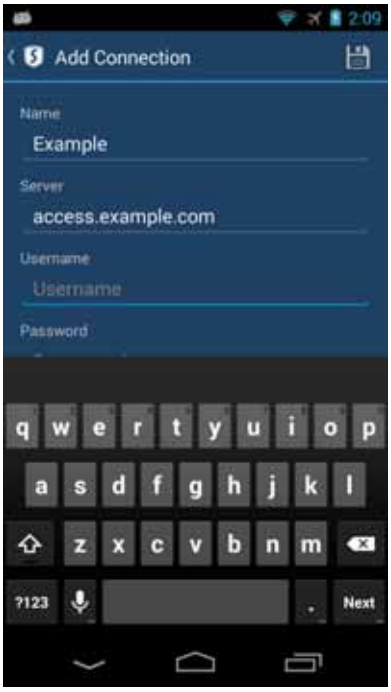
1. Launch SonicWALL Mobile Connect. You will be presented with the screen to begin your first connection. Tap **Add connection**.
   - **Name**: Enter a descriptive name for the connection.
   - **Server**: Enter the URL or IP address of the server.

2. Tap **Next**. Mobile Connect will then attempt to contact the Dell SonicWALL appliance.

If the attempt fails, a warning message will display, asking if you want to save the connection. Verify that the server address or URL is spelled correctly, and then tap **Save**.



3. If Mobile Connect successfully contacts the server, you will be prompted to enter your **Username** and **Password** (unless the server does not require this information).



Note If the screenshots above do not match what is displayed on your device, you are connecting to a Dell SonicWALL E-Class SRA or Dell Secure Mobile Access appliance. Proceed to Creating a Connection to Dell SonicWALL E-Class SRA Appliances on page 9.

4. The **Domain** field is auto-populated with the default domain from the server. To select a different domain, tap **Domain** to display a drop-down menu of the available options and tap **Save**.

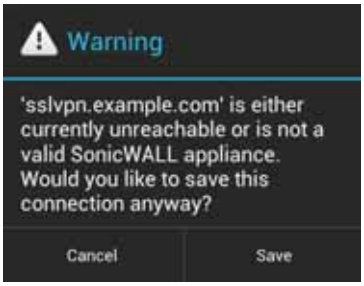
Creating a Connection to Dell SonicWALL E-Class SRA Appliances

In addition to full IPv4 support, VPN connections can connect to SRA EX appliances via IPv6 and can access IPv6 resources over the VPN. This feature requires 10.7.x E-Class SRA firmware or higher.

To connect to an E-Class SRA server:

1. Launch Mobile Connect. You will be presented with the screen to begin your first connection. Tap **Add connection**.
   - **Name**: Enter a descriptive name for the connection.
   - **Server**: Enter the URL or IP address of the server.

2. Tap **Next**. Mobile Connect will then attempt to contact the Dell SonicWALL appliance. If the attempt fails, a warning message will display, asking if you want to save the connection.



3. Before tapping **Save**, verify that the server address or URL is spelled correctly.

   If Mobile Connect successfully contacts the server, the connection will be automatically saved.

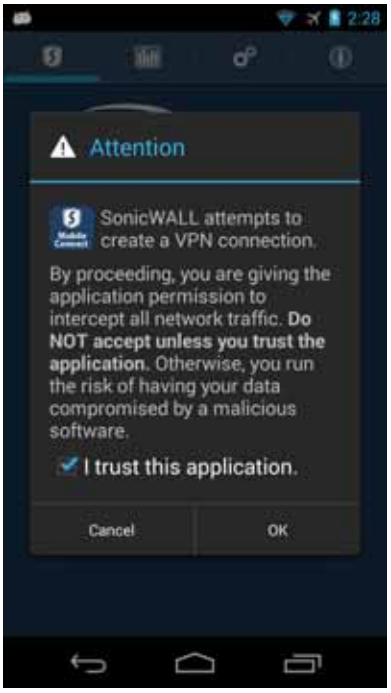
Connecting to the Mobile Connect Server

After you save a new connection, the list of all configured connections displays.

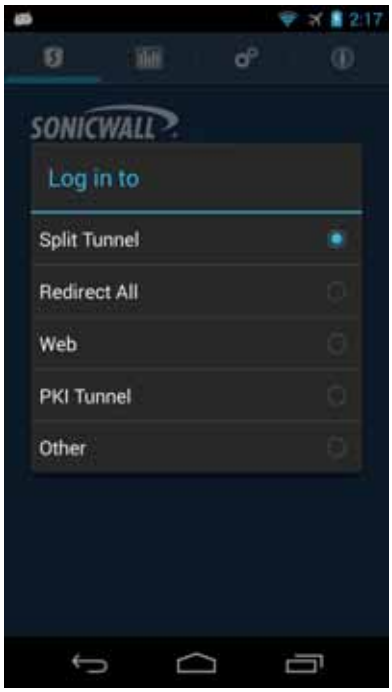
To establish a Mobile Connect session, perform the following tasks:

1. Tap the connection in the list that you want to initiate. The **Connection Status** page displays. Tap the **VPN ON/OFF** switch.

2. The first time you initiate a connection, a warning message displays. Tap the **I trust this application** checkbox, and then tap **OK**.

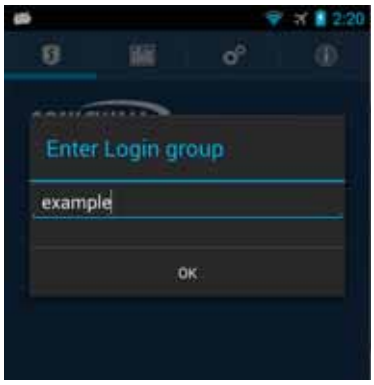


3. **For E-Class SRA connections only:** If Mobile Connect successfully contacts the server, you will be prompted to select which Login Group on the appliance you want to connect to. If you do not know which Login Group to connect to, contact your network administrator.



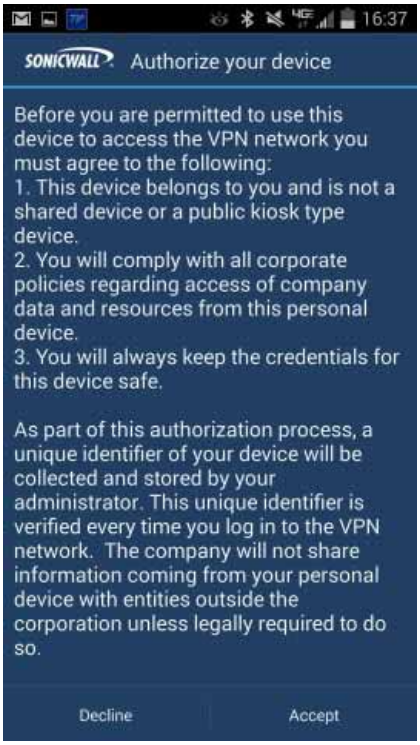
Note If the screenshots above do not match what is displayed on your device, you are connecting to a Dell SonicWALL firewall or SRA appliance. Proceed to Creating a Connection to Dell SonicWALL Firewall and SRA Appliances on page 7, step 3.

4. **For E-Class SRA connections only:** If the Login Group you connect to is not listed, select **Other...** to manually type in the group name.

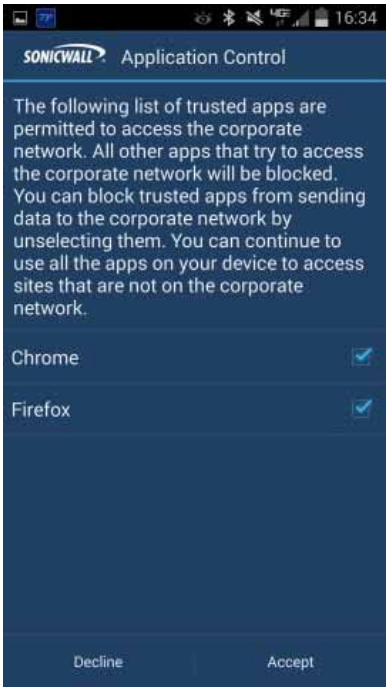


5. **For E-Class SRA connections only:** Enter your username and password if prompted (depending on whether the Dell SonicWALL appliance you are connecting to allows for saving usernames and passwords).

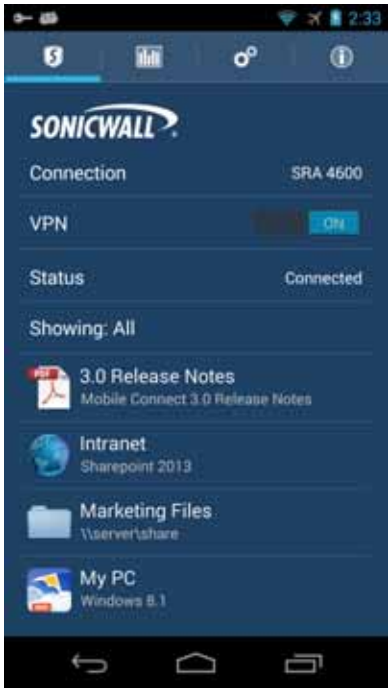
6. If this is the first time you have connected to an E-Class SRA server with Personal Device Authorization enabled, you are prompted to register your device. A similar prompt appears if the terms and conditions have changed. To continue, tap **Accept** to agree to the terms and conditions.



7. If connecting to an E-Class SRA server with Application Access Control configured, a notification about Data Privacy with a list of the applications under control is displayed. Optionally, uncheck any of the displayed apps if you are only using them for personal use and you do not want their traffic sent to the corporate network. Then tap **Accept** to accept the terms and continue.

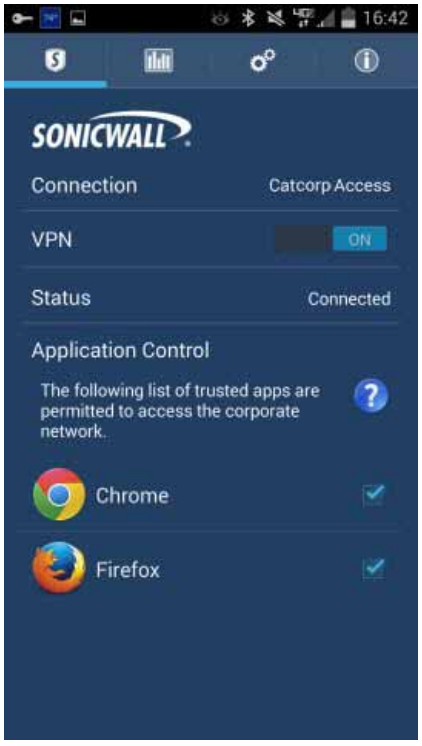


When the connection is successfully established, the **Status** changes to **Connected** and the VPN switch remains in the ON position.

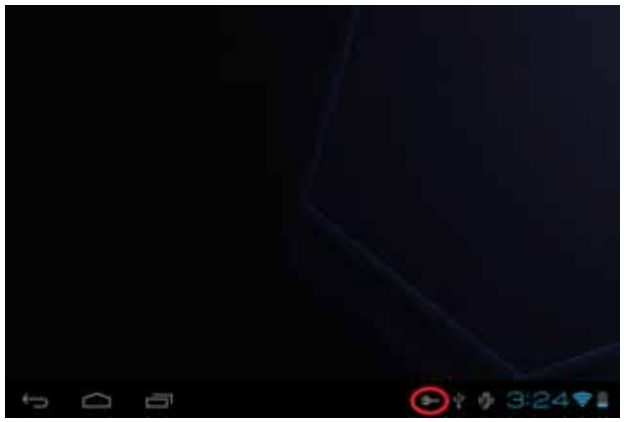


Any bookmarks defined for the portal are displayed below the Status line, and allow you to navigate directly to the bookmark's destination. Bookmarks will only appear after a VPN connection is established if the server is running firmware that supports Mobile Connect bookmarks and bookmarks have been defined for that user.

If Application Access Control is configured on the server (E-Class SRA only), the list of Bookmarks is replaced by a list of apps that are allowed to access the corporate network.



8. Press the **Home** button to return to your device's home screen. You can now navigate to other apps to access your Intranet network. The status bar will display a VPN icon to indicate that the session is still connected.

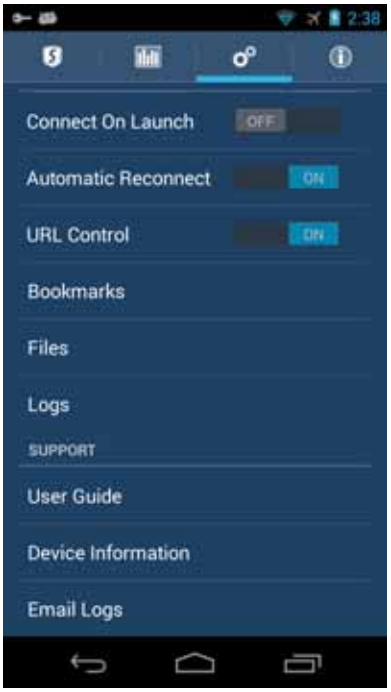


If the VPN connection is interrupted, the VPN icon will disappear and you will no longer be able to access the Intranet network. This can happen if your device's connection transitions to a different network connection (for example, from Wi-Fi to cellular).

Return to Mobile Connect to reestablish the connection. Optionally, you can configure the **Automatic Reconnect** option on the **Settings** tab to have Mobile Connect automatically attempt to reestablish interrupted connections.

Configuring Mobile Connect Settings

SonicWALL Mobile Connect provides several settings for connection and logging options. The Settings tab also provides Support information, which includes a User Guide and device, connection, and server information.



The following options are controlled from the Settings tab:

- **Connect on Launch** - Sets Mobile Connect to automatically initiate a connection to the last-used profile when it is launched.
- **Automatic Reconnect** - Sets Mobile Connect to automatically attempt to reconnect if the connection is lost. The SSL VPN connection can be disrupted when your device's connection transitions to a different network type (for example, from Wi-Fi to 3G). This setting lets applications rely on a sustained VPN connection. There is no limit on the amount of time it takes to reconnect.
- **URL Control** - Allows other mobile applications to pass action requests using special URLs to Mobile Connect. These action requests can create VPN connection entries and connect or disconnect VPN connections. For example, another application can launch Mobile Connect, access internal resources as needed, and then disconnect by using the **mobileconnect://** or **sonicwallmobileconnect://** URL scheme. Some common examples of URL Control are:

  Add profile: **mobileconnect://addprofile**[**/**]**?name=***ConnectionName***&server=***ServerAddress*[**&***Parameter1***=***Value***&***Parameter2***=***Value...*]

  Connect: **mobileconnect://connect**[**/**]**?[name=***ConnectionName*|**server=***ServerAddress*][**&***Parameter1***=***Value***&***Parameter2***=***Value...*]

  Disconnect: **mobileconnect://disconnect[/]**

  Additional information about URL Control is provided in URL Control Syntax and Parameters on page 18.

- **Bookmarks** - Displays centrally configured shortcuts (called bookmarks) to VPN resources like web pages, Remote Desktop servers, files, and terminal servers. These bookmarks, which are displayed on the main Connection tab when the VPN is connected, provide one-touch access to frequently used applications.

  If using a SRA appliance, pulling down the Connection screen and releasing it refreshes the bookmarks. Mobile Connect supports Remote Desktop options like screen size and enable/disable audio as long as both the server bookmark and third party application support the option.

  Note Bookmarks are supported on SRA appliances only when running 7.0 or higher and not supported on Next Generation Firewall appliances running SonicOS.

  Additional information about bookmarks is provided in Bookmarks.

- **Files > Delete Cached Files** - Deletes all cached files that have been downloaded and stored on the device. Note that cached files are stored encrypted on the device for added security.

  Note Files are supported on SRA appliances only when running 7.5 or higher and not supported on appliances running SonicOS.

  Additional information about Files is provided in Files Bookmarks.

- **Logs > Debug Logging** - Enables full debug log messages of Mobile Connect activity. Leave this setting disabled unless instructed to enable it by Dell SonicWALL Support staff.
- **Logs > Clear Logs** - Deletes all log files saved on the device.

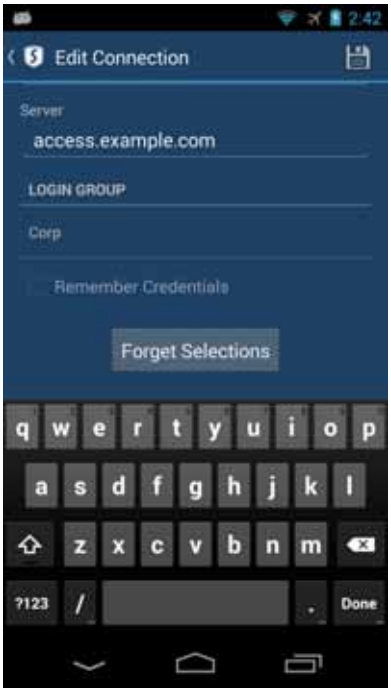
The **Support** section of the Settings tab provides the following support information:

- **User Guide** - Displays the SonicWALL Mobile Connect User Guide.

- **Device Information** - Displays information about the device, Wi-Fi connection, Cellular connection, and DNS servers.
- **Email Logs** - Creates an email to send the Mobile Connect log to Dell SonicWALL Support staff. Tap **Send** to send the email.

E-Class SRA Settings

Connections to Dell SonicWALL E-Class SRA appliances have two additional options that are available on the **Edit Connection** window. To view this option, go to the **Connection** tab and tap and hold on the Connection line to bring up the **Edit Connection** window.



The following options can be configured:

- **Remember Credentials** - Enables saving of user authentication credentials for the VPN connection. This is enabled by default and can be controlled by the E-Series SRA server setting. This feature requires E-Class SRA 10.7.x or Dell Secure Mobile Access 11.0 (or higher) firmware.
- **Forget Selections** - Mobile Connect remembers the Login Group that you specified when configuring the connections. To change to a different Login Group, tap **Forget Selections**. The next time you connect to the server, you will be prompted to select a new Login Group.

Note: If this option is not displayed, you are connecting to either a Dell SonicWALL firewall or SRA appliance.

URL Control Syntax and Parameters

This section provides the full set of URL parameters for the URL Control feature. URL Control currently supports the addprofile, connect, and disconnect commands. Callback URLs are also supported.

Add Profile Command

The addprofile command requires either the name or server parameter, and accommodates both. All other parameters are optional. When the URL is opened in Mobile Connect, all of the parameters included in the URL are saved in the connection entry associated with that name and server.

Syntax:

`mobileconnect://addprofile[/]?name=`*`ConnectionName`***`&server=`***`ServerAddress`**
`[&`***`Parameter1`***`=`***`Value`***`&`***`Parameter2`***`=`***`Value...`***`]`

Following are examples of the addprofile command:

```
mobileconnect://addprofile/?name=Example&server=vpn.example.com
sonicwallmobileconnect://addprofile/?name=Example&server=vpn.example.com
mobileconnect://addprofile?name=Example%202&server=vpn.example.com
mobileconnect://addprofile?name=vpn.example.com
mobileconnect://addprofile?server=vpn2.example.com
mobileconnect://addprofile?name=SRA%20Connection&server=sslvpn.example.com&
username=test&password=password&domain=LocalDomain&connect=1
mobileconnect://addprofile?name=EX%20Connection&server=workplace.example.com&
username=test&password=password&realm=Corp&connect=1
```

Note: All appropriate characters in values of parameters used in URLs are required to be URL encoded. For instance, to match a space, enter %20.

Add Profile Command Parameters

Command Parameter	Description
`name`	The unique name of the VPN connection entry that will be created and appear in the Mobile Connect Connections list. Mobile Connect accepts the name only if it is unique. Letters are case sensitive.
`server`	The domain name or IP address of the Dell SonicWall appliance in which you wish to connect. For example: `vpn.example.com`
`username`	**Optional**: The username used in the VPN connection.
`password`	**Optional**: The password used in the VPN connection.
`realm`	**Optional**: The realm used in the VPN connection profile. Applies to EX series connections only.
`domain`	**Optional**: The domain used in the VPN connection profile. Applies to SRA and UTM connections only.
`sessionid`	**Optional**: The session ID or Team ID used for authentication.
`connect`	**Optional**: If presented and the value is non-null, the connection will be initiated if the profile was successfully added.
`callbackurl`	**Optional**: The callback URL is be opened by Mobile Connect after the add profile command has been processed. See Add Profile Command on page 19 for full details of the callback URL syntax and options.

Connect Command

The connect command is used to easily establish VPN connections. Connection information can be embedded in the URLs and they can be provided to users for easy setup and configuration. In addition, a callback URL can be provided that Mobile Connect will open after the connection attempt is completed, making it possible for other applications to initiate VPN connections in a seamless manner.

Syntax:

mobileconnect://connect[/]?[name=*ConnectionName***|server=***ServerAddress***]** [**&***Parameter1***=***Value***&***Parameter2***=***Value...***]**

Following are examples of the mobileconnect command:

```
mobileconnect://connect/?name=Example
sonicwallmobileconnect://connect/?name=Example
mobileconnect://connect?name=Example
mobileconnect://connect?server=vpn.example.com
mobileconnect://connect?name=Example%202&server=vpn.example.com
mobileconnect://
connect?name=SRA%20Connection&server=sslvpn.example.com&username=test
&password=password&domain=LocalDomain
mobileconnect://connect?name=EX%20Connection&server=
workplace.example.com&username=test&password=password&realm=Corp
```

Connect Command Parameters

Command Parameter	Description
`name`	The unique name of the VPN connection entry that will be created and appear in the Mobile Connect Connections list. Mobile Connect accepts the name only if it is unique. Letters are case sensitive.
`server`	The domain name or IP address of the Dell SonicWall appliance in which you wish to connect. For example: `vpn.example.com`
`username`	**Optional**: The username used in the VPN connection.
`password`	**Optional**: The password used in the VPN connection.
`realm`	**Optional**: The realm used in the VPN connection profile. Applies to EX series connections only.
`domain`	**Optional**: The domain used in the VPN connection profile. Applies to SRA and UTM connections only.
`sessionid`	**Optional**: The session ID or Team ID used for authentication.
`connect`	**Optional**: If presented and the value is non-null, the connection will be initiated if the profile was successfully added.
`callbackurl`	**Optional**: The callback URL is be opened by Mobile Connect after the connect command has been processed. See Connect Command on page 20 for full details of the callback URL syntax and options.

Disconnect Command

The `disconnect` command is used to disconnect an active connection. In addition, a callback URL can be provided that Mobile Connect will open after the connection is disconnected, which makes it possible to return to the calling app. If there is no active VPN connection, the command is ignored.

Syntax:

```
mobileconnect://disconnect[/]
mobileconnect://disconnect[/]?[callbackurl=<callbackurl>]
```

Following are examples of the disconnect command:

```
mobileconnect://disconnect
```

```
mobileconnect://disconnect/
```

```
sonicwallmobileconnect://disconnect
```

```
mobileconnect://
disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%
26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
```

```
sonicwallmobileconnect://
disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%
26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
```

Disconnect Command Parameters

Command Parameter	Description
`callbackurl`	**Optional**: The callback URL is opened by Mobile Connect after the disconnect command has been processed. See Disconnect Command on page 21 for full details of the callback URL syntax and options.

Callback URL

While invoking Mobile Connect using a URL, a third party application can include a callback URL that is called by Mobile Connect once it completes the requested action. The callback URL value may also contain special tokens that will be evaluated and dynamically replaced by Mobile Connect to provide additional status and connection information back to the app that is opened by the callback URL. Tokens are evaluated in place, in the same order in which the tokens were specified.

To ensure that it functions properly, the base callback URL format should be RFC 1808 compliant and should be able to be launched independently of Mobile Connect. For example it should launch through a web page or iOS web clip.

`URL: <scheme>://<net_loc>/<path>;<params>?<query>#<fragment>`

Note The value of callbackurl must also be properly URL encoded to ensure that Mobile Connect can process the callback URL correctly.

Dynamic Tokens Supported by the Callback URL

Dynamic Token	Description
`$ERROR_MESSAGE$$`	The string value of the error message from the failed connection attempt.
`$LOGIN_GROUP$`	The string value of the authentication login group or realm. Applies to EX series connections only.
`$COMMUNITY$`	The string value of authentication community. Applies to EX series connections only.
`$ZONE$`	The string value of EPC zone. Applies to EX series connections only.
`$TUNNEL_IP$`	The string value of the Mobile Connect IPv4 client address.
`$TUNNEL_MODE$`	One of split, split-nonlocal, redirectall, or redirectall-nonlocal depending on the tunnel mode. Applies to SRA and UTM connections only.
`$ESP_ENABLED`	Yes, or no depending on if ESP is enabled. Applies to SRA and UTM connections only.

Note Any number of tokens from the table above can be specified.

Following are examples using the callback URL:

Callback URL
```
customapp://host?status=$STATUS$&login_group=$LOGIN_GROUP&
error_code=$ERROR_CODE$
```

Full URL with URL Encoded Callback URL Value
```
mobileconnect://connect?sessionid=<teamid>&callbackurl=customapp%3A%2F%
2Fhost%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%
26error_code%3D%24ERROR_CODE%24
```

Callback URL
```
myapp://callback?status=$STATUS$&login_group=$LOGIN_GROUP&
error_code=$ERROR_CODE$
```

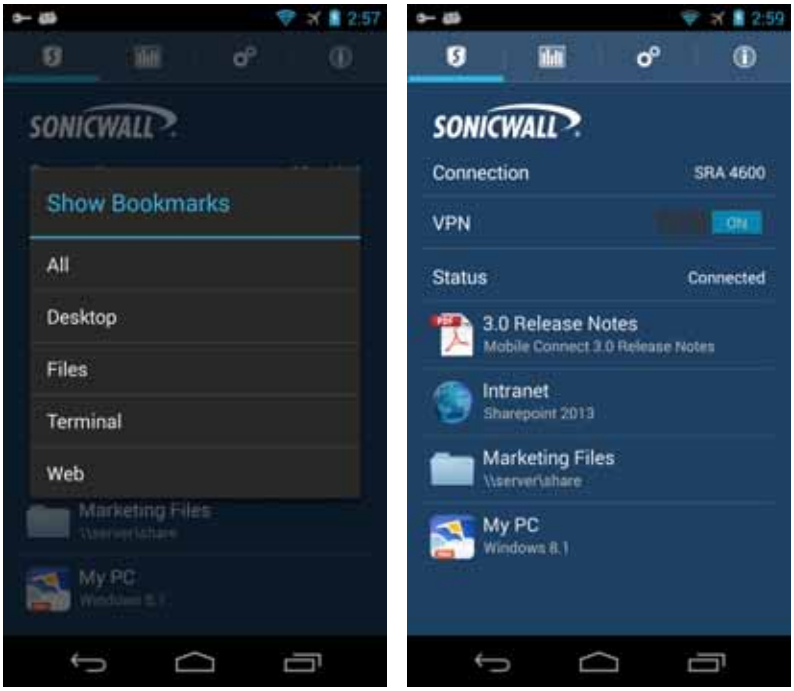
Full URL with URL Encoded Callback URL Value
```
mobileconnect://connect?sessionid=<teamid>&callbackurl= myapp%3A%2F%
2Fcallback%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%
26error_code%3D%24ERROR_CODE%24
```

Callback URL
```
http://server/example%20file.html
```

Full URL with URL Encoded Callback URL Value
```
mobileconnect://connect?callbackurl=http%3A%2F%2Fserver%2Fexample%2520file.html
```

Bookmarks

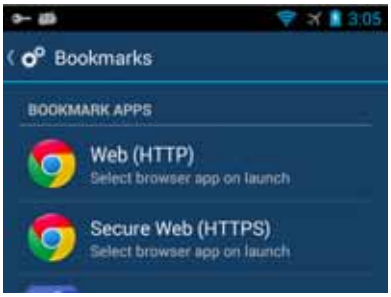
When there are more than five bookmarks, the bookmarks are replaced by a Filter screen that groups bookmarks by type. Select the type of bookmarks to display or select **All Bookmarks** to display all bookmarks.



Note When connected to an SMB SRA server, SRA 7.0 or higher is required for Bookmarks support.

Note When connected to a Dell Secure Mobile Access appliance with Application Access Control enabled, the Bookmarks list is replaced by a list of trusted apps that can access the corporate network.

Selecting a bookmark for an app that is not installed will prompt you to install the app. Apps referenced by bookmarks also can be installed at any time using the **Settings > Bookmarks** tab. In addition to installing apps for bookmarks, the **Settings > Bookmarks** tab is also used to select and install apps for bookmarks that support multiple third party apps. For example, you might select Chrome or Firefox for a Web bookmark.



Mobile Connect supports the following types of bookmarks and associated apps.

Desktop Bookmarks:

Portal name: Terminal Services (RDP – ActiveX), Terminal Services (RDP – Java) Internal type: RDP5ActiveX, RDP5Java

RDP bookmark types attempt to launch with the associated RDP application, as configured in the Settings tab.

	Android Version
Wyse PocketCloud Pro	1.4.217
2X Client RDP/Remote Desktop	11.0.1899
Remote RDP Lite	4.2.8
Remote RDP	4.2.8
Remote RDP Enterprise	4.2.8
Microsoft Remote Desktop	8.0.5

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters will vary based on the application. For example:

- Wyse PocketCloud Pro does not support the “connect to console” option

Portal name: Virtual Network Computing (VNC)
Internal type: VNC

VNC bookmark types attempt to launch with the associated VNC application as configured in the Settings tab.

	Android Version
Wyse PocketCloud Pro	1.4.217
android-vnc-viewer	0.5.0

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters varies based on the application.

Portal name: Citrix Portal (Citrix)
Internal type: Citrix, Citrix_https

Citrix bookmark types will attempt to launch with the associated Citrix application.

	Android Version
Citrix Receiver	3.4.13

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters will very based on the application.

Web Bookmarks:

Portal name: Web (HTTP), Secure Web (HTTPS), External Web Site
Internal type: HTTP, HTTPS, URL, URL_https

These bookmarks will launch in an associated web browser and the provided 'Name or IP Address' (HostID) will be passed as the parameter to display in the browser.

	Android Version
Any Browser	Yes
Google Chrome	33.0.1750.170

Portal name: Mobile Connect
Internal type: MC

The Mobile Connect bookmark type will rely on the operating system to determine and launch the proper application. The bookmark is expected to be properly configured for launch. The Mobile Connect app will attempt to launch it as is. (for example, telnet://server)

Terminal Bookmarks:

Portal name: Telnet, Secure Shell Version 1 (SSHv1), Secure Shell Version 2 (SSHv2)
Internal type: Telnet, SSH, SSHv1

	Android Version
ConnectBot	1.7.1

ConnectBot notes: Proper formatting is required for ConnectBot SSH (server bookmark field requires username@server).

Note Some supported third party apps may not yet be available in the Amazon Appstore.

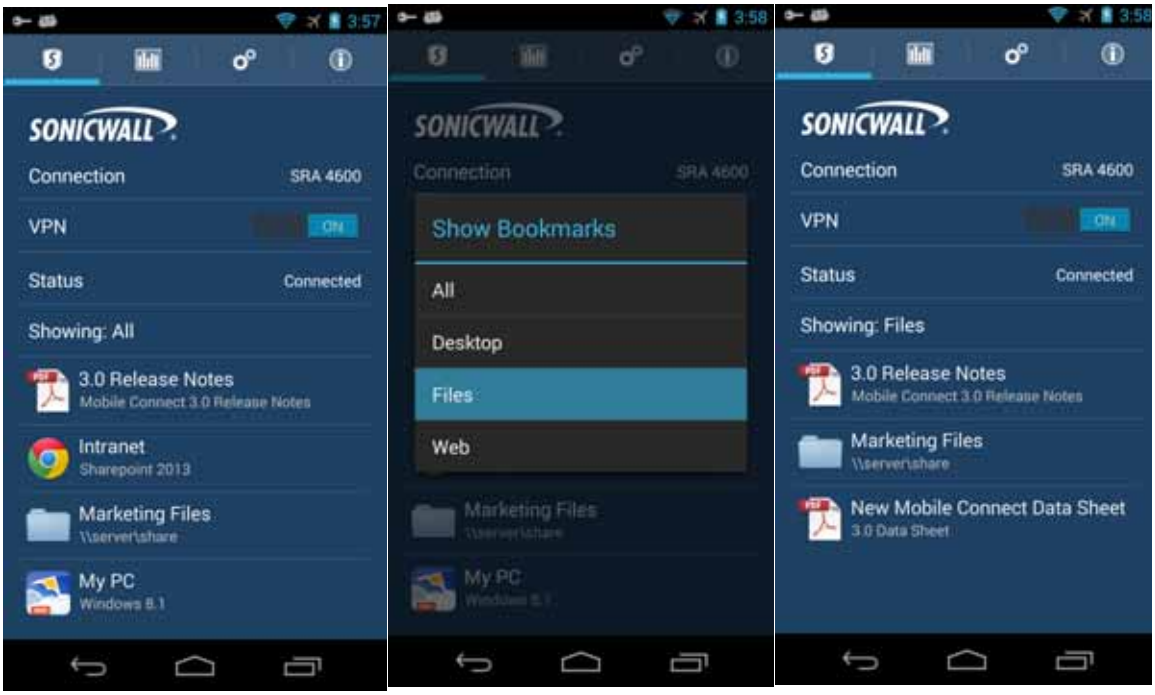
Files Bookmarks

Mobile Connect 3.0 introduced secure mobile access to files through Files bookmarks. Files bookmarks are displayed after the VPN is connected in the table of bookmarks. Tapping a Files bookmark allows secure access to files by first checking and enforcing the server-configured file policy, and then securely downloading and displaying the file within the Mobile Connect app.

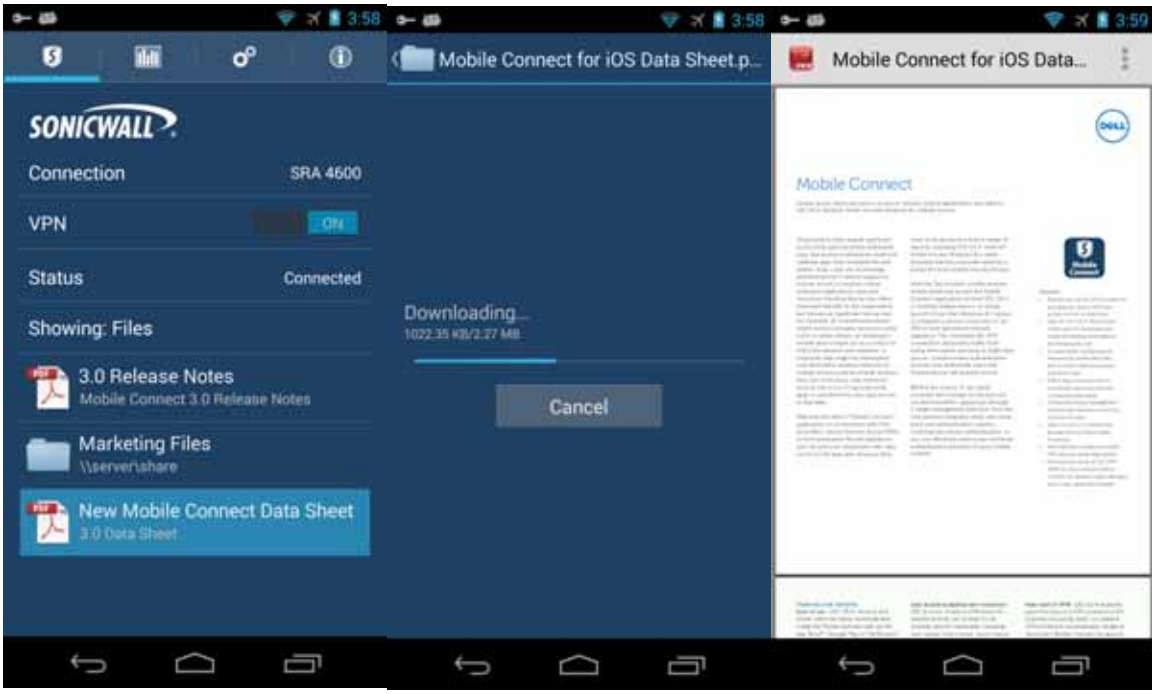
Granular policy controls can be configured to allow other Android apps to use each file. On Android, policies include control over whether a file may be opened in a third-party app or securely cached on the device. Files bookmarks can also be created to folders or file share root directories to allow directory navigation.

Note Beginning in Mobile Connect for Android 3.0, Files bookmarks are supported on the Dell SonicWALL SRA appliances starting with SRA 7.5 firmware. Support for Files bookmarks in Dell Secure Mobile Access and Next Generation Firewalls is expected in a future release.

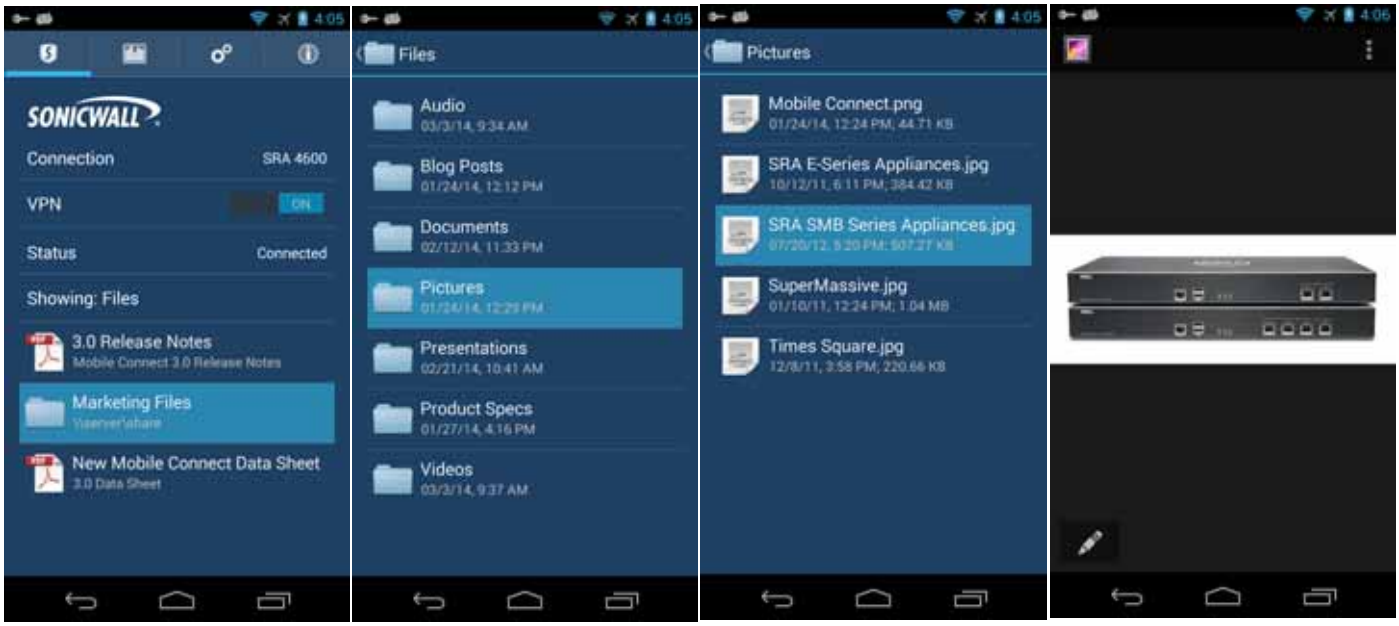
When Files bookmarks are configured for the user on the server appliance, they appear in the list of bookmarks after the VPN is established and can be filtered by selecting the **Showing: Files** row that is displayed when there are more than five bookmarks.



Tapping a Files bookmark queries and enforces the server-configured file policy for that file bookmark. If the file is not already cached on the device, it securely downloads the file from the SRA appliance. Once the file is downloaded, it is opened in the Android default file viewer app for that file type.



Tapping a Files bookmark to a folder or directory allows for directory browsing and file download and viewing of any file in the folder. All attempts to browse a file folder or view a file query the server to enforce access policies. On Android, the default file viewer app is automatically launched after a file is downloaded.



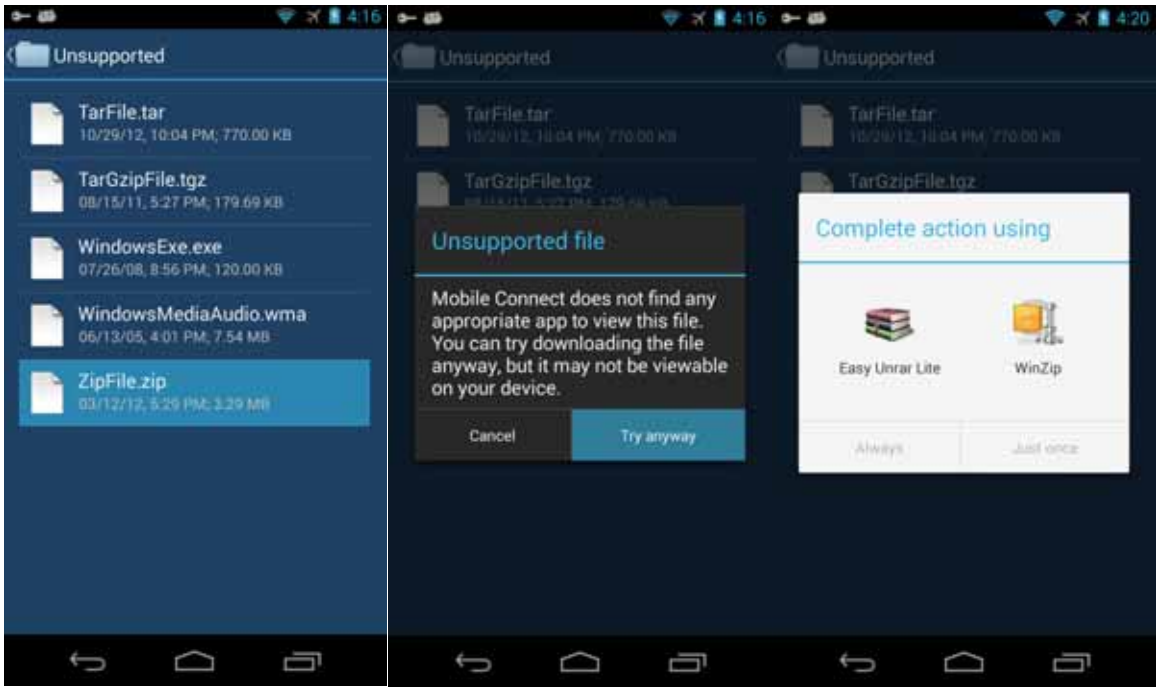
Supported File Types

Mobile Connect supports all file types natively supported by Android, including the following:

	File Extension
Images	.jpg, .jpeg, .tif, .tiff, .png
Music	.mp3, .m4a, .wav
Movies	.mov, .mp4
Microsoft Word Documents	.doc, .docx
Microsoft Excel Spreadsheets	.xls, .xlsx
Microsoft Powerpoint Presentations	.ppt, .pptx
Adobe PDF	.pdf
Web Pages	.htm, .html
Text and Rich-text Files	.txt, .rtf

Unsupported Files

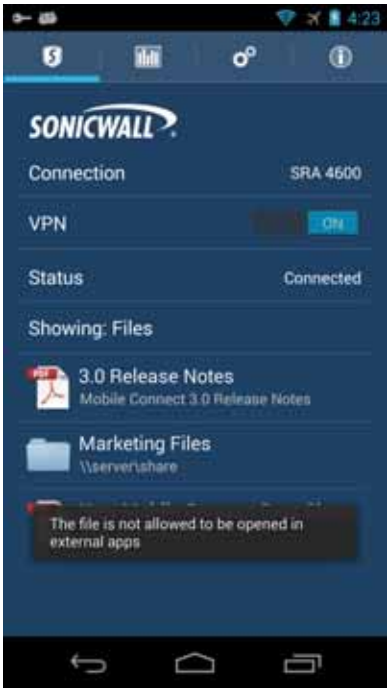
If a file type is not supported, the user will be prompted that the file may not be viewable unless there is another app installed that can view the file. The user can tap ‘Try Anyway’ and if there is another app that is registered to handle that file type, the user will have the option to open the file in that app.



File Policies

On Android, server-configured policies control whether a file can be opened in a third-party app or securely cached on the device.

For example, if a file has the *Allow Open In* policy disabled, the file cannot be viewed on an Android device. Mobile Connect launches third-party apps to view all file types, so the *Allow Open in* policy must be enabled to view a file.



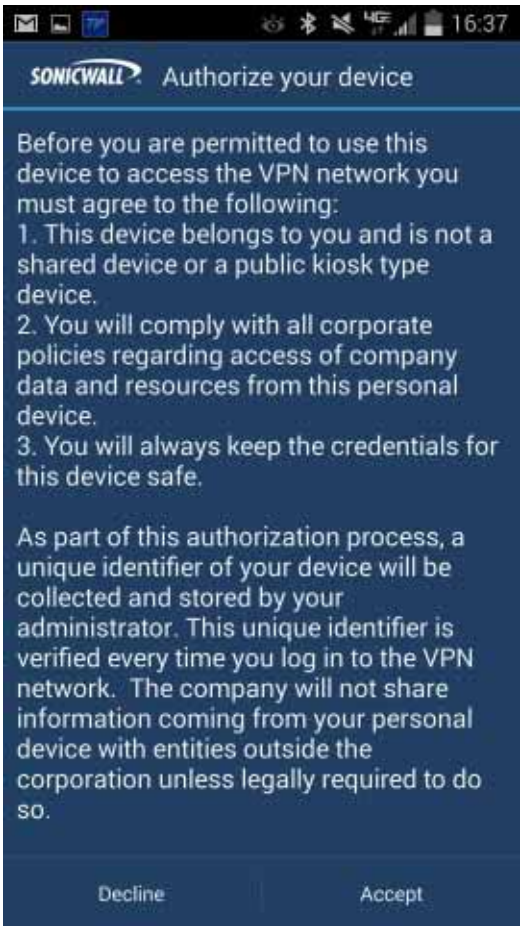
Application Access Control

Mobile Connect 3.1 supports the Application Access Control feature in Dell Secure Mobile Access 11.0 and higher on E-Class SRA appliances. Application Access Control allows remote access administrators to control exactly which resources on the corporate network each application (app) can access. Meanwhile, the device owner can still use their personal Android device for their own activities such as personal email, financial data, pictures, music, accessing third party web sites, etc.

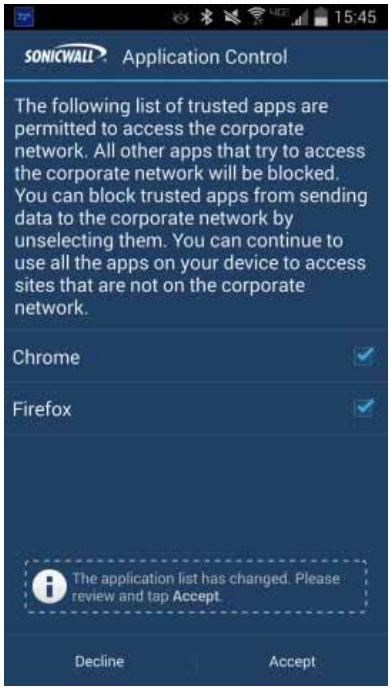
If the E-Class SRA administrator has configured this feature, you will log in to a Login Group that allows a list of trusted apps to access corporate resources. The specific version of each app is included in the configuration. The Application Access Control rule list controls:

- Which applications can send data through the VPN tunnel
- Which destinations on the corporate network those applications are allowed to access

The first time you connect and log in, you must agree to the displayed terms and conditions.

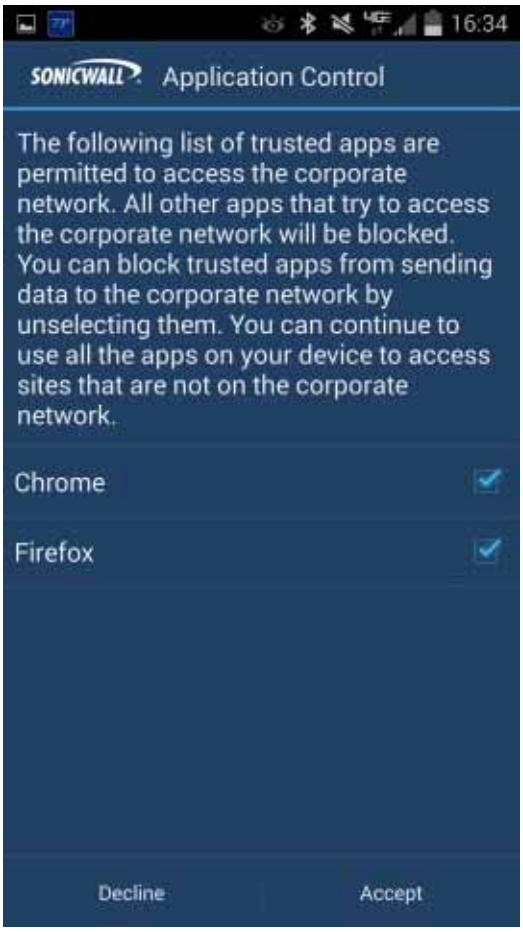


Your device is then registered with the server, and will be recognized in later connections. If the policy or list of trusted apps changes, you will be asked to re-accept the terms and conditions.

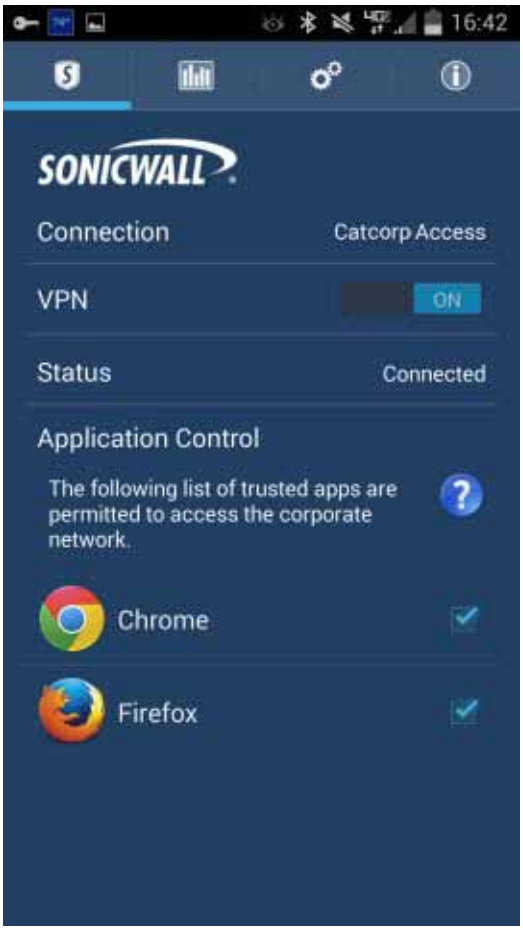


Multiple personal devices can be authorized for a single user, and a single personal device may be registered by multiple users.

The list of trusted apps is displayed on your device after you agree to the above terms. You can block trusted apps from sending data to the corporate network by clearing the checkbox for them on your device. Typically, you would uncheck any application that is only being used for personal tasks or information, to prevent the app from sending any traffic to the corporate network. Tapping **Accept** continues with the connection.

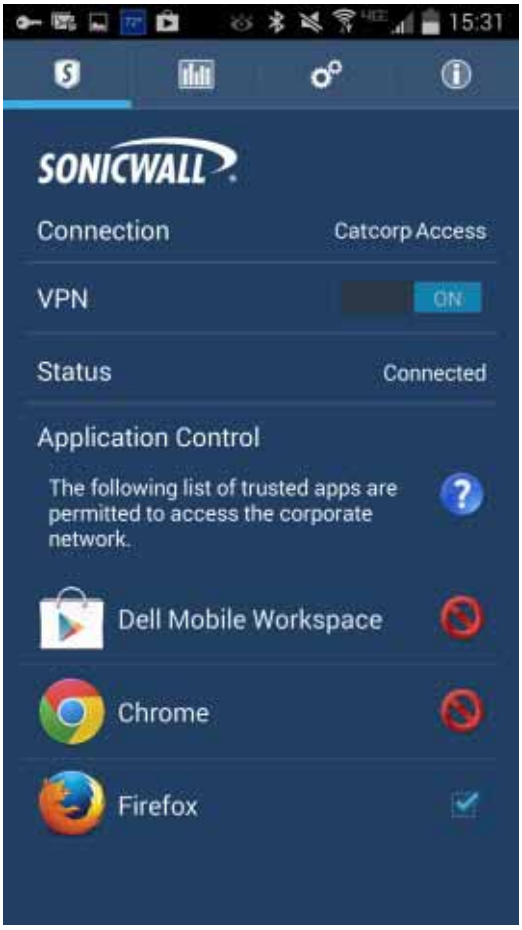


The device is now fully connected to the E-Class SRA server.



To request that additional apps be added to the trusted apps list, contact the E-Class SRA appliance administrator.

If your device has an app installed that is not the same version as the one approved on the server, or if an approved app is not installed on your device, the app name is displayed without a check mark. Instead, a red circle “no” symbol is displayed next to it.



When connected to an E-Class SRA server running Dell Secure Mobile Access 11.0 or higher with Application Access Control configured, device traffic is handled in three ways:

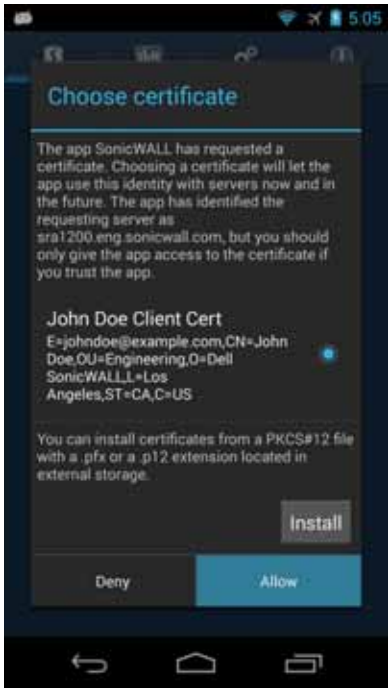
1. For applications listed and selected in the application list, traffic destined for the corporate network from those applications is allowed to enter the VPN tunnel. The application ID and signature are used by the server to identify the application.
2. For applications which are on that list and are *not* selected (or any other application on the device), traffic destined for the corporate network is blocked and/or dropped by Mobile Connect and does NOT enter the tunnel.
3. All applications (regardless of whether or not they are on the application list) send traffic out the default interface of the device if the traffic is NOT destined for the corporate network.

Configuring Client Certificates

Note Client certificate support is only available for connections to Dell SonicWALL E-Class SRA, Dell Secure Mobile Access, and SMB SRA appliances.

Configuring Client Certificates with E-Class SRA Appliances

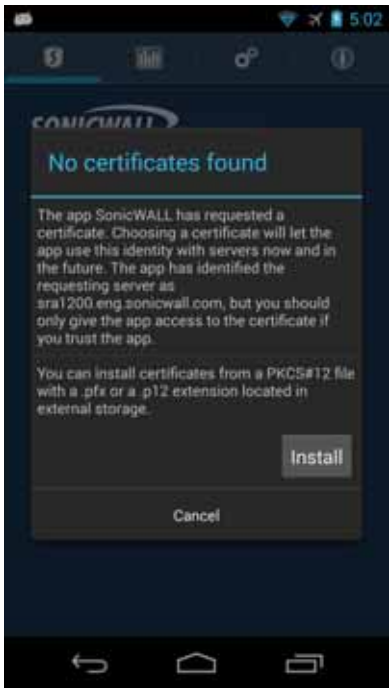
If a client certificate is required during authentication, you are automatically prompted to select a client certificate from the Android device client certificate store.



Select the client certificate from the list of certificates and tap **Allow**.

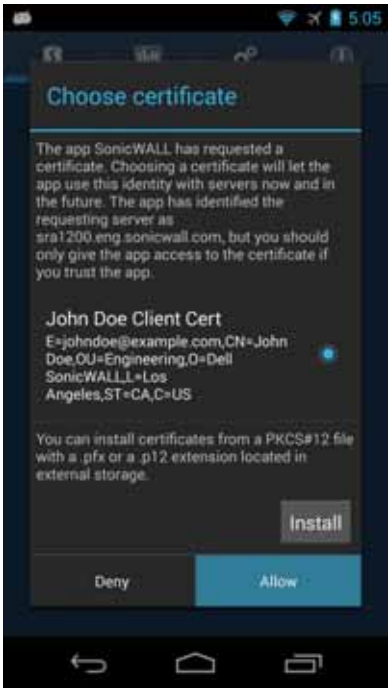
By default a VPN configuration prompts you to select the client certificate during authentication. If you successfully authenticate with a client certificate, the VPN configuration profile is automatically updated to use the client certificate for each subsequent connection attempt. To reset the client certificate selection, edit the connection and tap the **Forget Selections** button.

Note If no client certificates are installed, an Android *No certificates found* dialog appears with an option to install a PKCS#12 file located in external storage.



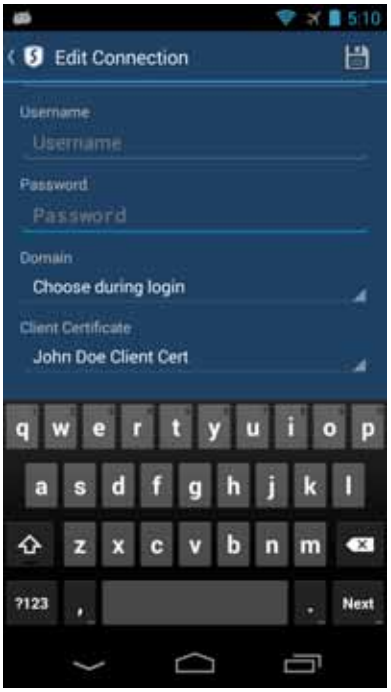
Configuring Client Certificates with SMB SRA Appliances

On Dell SonicWALL SMB SRA appliances, client certificate authentication is available as a second factor authentication method in addition to standard user name and password authentication. If a client certificate is required during authentication, you are automatically prompted to select a client certificate from the Android device client certificate store.



Select the client certificate from the list of certificates and tap **Allow**.

By default the client certificate is set to **Choose during login** for a VPN configuration. If you successfully authenticate with a client certificate, the VPN configuration profile is automatically updated to set the client certificate to the one that was chosen. To reset the client certificate selection, edit the connection and set the Client Certificate field back to **Choose during login**.

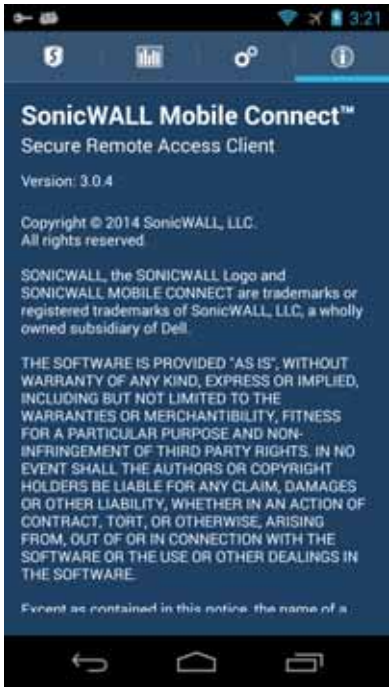


Note If no client certificates are installed, an Android *No certificates found* dialog appears with an option to install a PKCS#12 file located in external storage.

Monitoring Mobile Connect

The **Monitor** tab displays additional details about the connection, statistics on traffic transmitted, DNS information, and routes that have been installed. The compression ratio is shown when connected to an appliance running SRA 7.5 or higher with compression enabled. Traffic over the VPN tunnel is compressed using the LZ4 algorithm.

The **About** tab of SonicWALL Mobile Connect displays the version number and legal text.



When a Mobile Connect session is active, the Android System Notifications area includes an entry indicating that the VPN is connected.

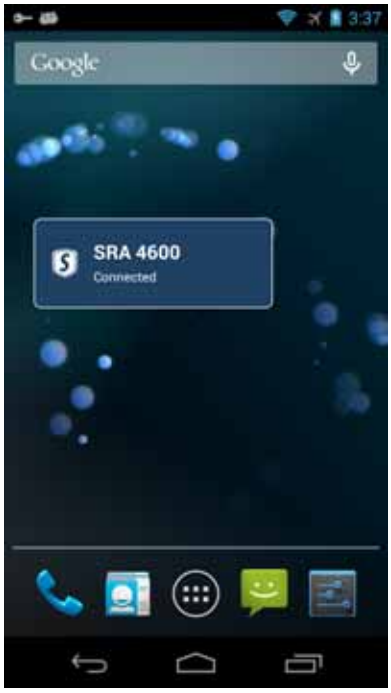
Tapping on the SonicWALL Mobile Connect entry in the Android System Notifications area displays a summary of statistics on the VPN session. The statistics page displays the server name, duration of the session, and the amount of traffic that has been sent and received. Three buttons are also provided on this screen:

- **Cancel** – Closes the statistics screen.
- **Disconnect** – Disconnects the Mobile Connect session.
- **Configure** – Launches the SonicWALL Mobile Connect app.

Mobile Connect Widget

When the SonicWALL Mobile Connect app is installed, a widget for Android is also created in the widgets tab. It can then be dragged from the widgets tab to the home screen. This widget is used as follows:

- The widget shows the connection status (connected, disconnected, connecting, etc.)
- Tap the icon to establish a tunnel when disconnected.
- Tap the icon to disconnect the tunnel when connected.
- Tap any other area of the widget to launch the Mobile Connect client.

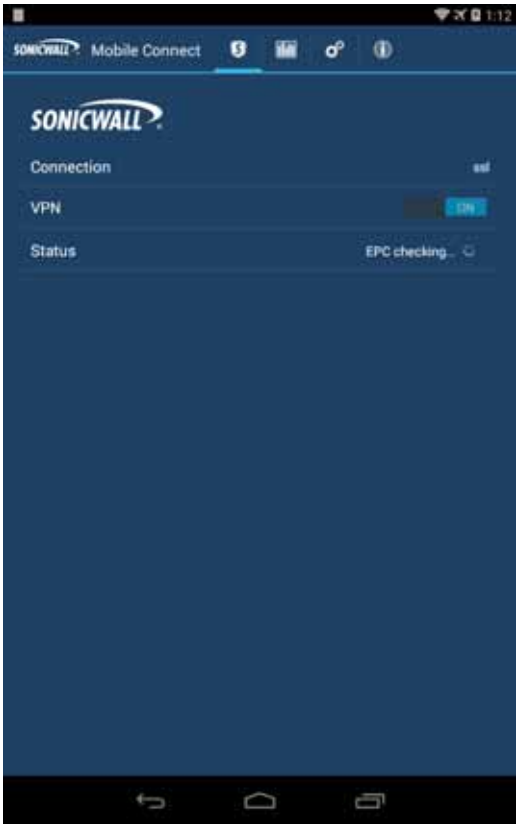


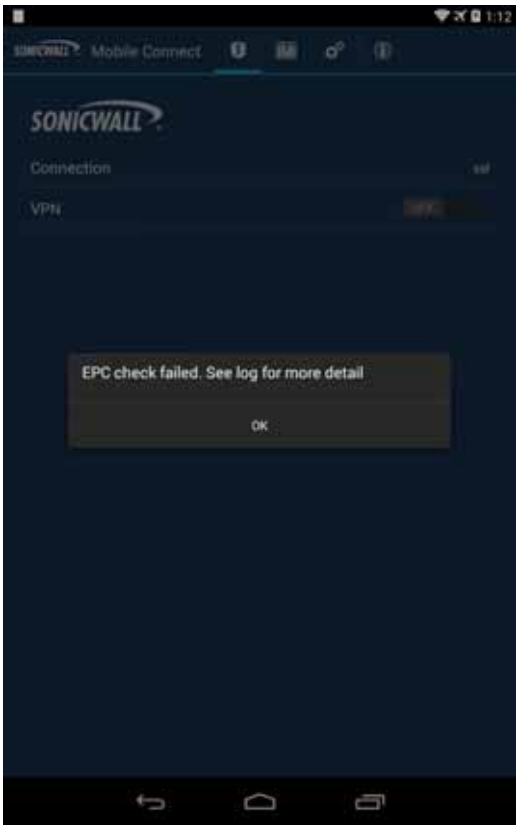
Troubleshooting Mobile Connect

This section describes some troubleshooting you can try if you are unable to connect to the Dell SonicWALL server.

Failed End Point Control Check

End Point Control can prevent the connection when the server is an E-Class SRA appliance or an SMB SRA appliance running SRA 7.5 (or higher). During the connection process, the connection status displays “EPC checking...” while the End Point Security policy checks are performed. If the device is not compliant because a security check failed, an error message is then displayed.





You can view the Mobile Connect log for more detailed information about which check failed. For example, you might see the following if an EPC policy was set up to restrict access to only a single device ID (EQUIPMENT ID).

```
2014-07-10 13:08:23:974 DEBUG Thread-142 - SraEpcManager - Allow Profile:
{AndroidEPCExamplePolicy:[Literal=EQUIPMENTID,1,1234567890]}

2014-07-10 13:08:23:976 DEBUG Thread-142 - SraEpcManager - Deny Profile: {}

2014-07-10 13:08:23:977 DEBUG Thread-142 - SraEpcManager - Recurring Mode: 1

2014-07-10 13:08:23:978 DEBUG Thread-142 - SraEpcManager - Recurring Period: 1

2014-07-10 13:08:24:200 DEBUG Thread-142 - SraEvaluator - Evaluate literal:
Literal=EQUIPMENTID,1,1234567890

2014-07-10 13:08:24:200 DEBUG Thread-142 - SraEvaluator - DeviceID<abcda50e-
e13b-1234-b89d-b3da7384a2f5>, expect<1234567890>
```

```
2014-07-10 13:08:24:201 INFO Thread-142 - SraEpcManager - Failed allow
profile:Literal=EQUIPMENTID,1,1234567890
```

When the server is either an E-Class SRA appliance or an SMB SRA appliance running SRA 7.5 (or higher), policies can be created to check different attributes of the Android device, including:

- Rooted or Not Rooted
- Client certificate installed
- Android OS version
- Device ID / Equipment ID
- Anti-Virus App
- Personal Firewall App
- Application
- Directory name
- File name

See the *Administrator Guide* for the server for complete information about End Point Control policy options.

General Troubleshooting

If you are unable to connect to the Dell SonicWALL server, perform the following steps to troubleshoot the connection.

1. Double check that you have entered the server name properly in the connection configuration.
2. Go to the web browser on your device and attempt to navigate to the SSL VPN appliance web portal.
3. If you are unable to load the web portal, the problem is with the Dell SonicWALL appliance. Contact your network administrator if the problem persists.
4. If the web portal loads successfully on the browser and you still cannot establish a Mobile Connect connection, notify Dell SonicWALL Support, as follows:
   a. On the **Settings** tab, enable the **Debug Logging** option.
   b. Attempt a connection to the server again to ensure that full debugging messages are logged for the attempt.
   c. Then return to the **Settings** tab and tap the **Email Logs** button. An email will launch in your mail client with the Mobile Connect log attached. Address the email to **Support@sonicwall.com**. Add any additional comments to the email and tap **Send**. Dell SonicWALL Support staff will contact you after reviewing your case.

Support Information

The following sections provide Dell SonicWALL Technical Support and End User License Agreement Information.

Contact Information

For timely resolution of technical support questions, visit Dell SonicWALL on the Internet at:

<http://www.sonicwall.com/us/support.html>. Web-based resources are available to help you resolve most technical issues or contact Dell SonicWALL Technical Support.

Technical Support Contact Information:

Contact Support Page - http://www.sonicwall.com/us/support/contact.html

Contact SonicWALL Page - http://www.sonicwall.com/us/company/286.html

End User Licensing Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SONICWALL PRODUCT. BY INSTALLING OR USING THE SONICWALL PRODUCT, YOU (AS THE CUSTOMER, OR IF NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) INDICATE ACCEPTANCE OF AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT FOR AND ON BEHALF OF THE CUSTOMER. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN DO NOT USE THE PRODUCT AND RETURN IT TO THE PLACE OF PURCHASE WITH PROOF OF PURCHASE WITHIN THIRTY (30) DAYS OF PURCHASE FOR A REFUND. IF YOU DO PROCEED TO INSTALL OR USE THE SONICWALL PRODUCT, YOU WILL HAVE INDICATED ACCEPTANCE AND AGREEMENT WITH THE TERMS AND CONDITIONS HEREIN. NOTWITHSTANDING THE FOREGOING, THIS AGREEMENT SHALL NOT SUPERSEDE ANY OTHER SIGNED AGREEMENT BETWEEN YOU AND SONICWALL THAT EXPRESSLY GOVERNS THE SONICWALL PRODUCT.

"Product" means the SonicWALL labeled hardware and related documentation ("Hardware") and/or proprietary SonicWALL labeled software, firmware and related documentation ("Software") purchased by the end user of the product either directly from SonicWALL or a Reseller (“Customer”). “Services” means the Support Services described below and any other services provided with or for the Products directly by SonicWALL or its agents. “Reseller” shall mean those entities to which SonicWALL or SonicWALL’s authorized distributors distribute the Products for resale to end users. Except as otherwise agreed upon by the parties, this Agreement will also cover any updates and upgrades to the Products provided to Customer by SonicWALL directly or through a Reseller (except as may be otherwise indicated, such updates and upgrades shall be deemed Products).

1. LICENSE(S) AND RESTRICTIONS

(a) Licenses. Subject to the terms and conditions of this Agreement, SonicWALL grants to Customer, and Customer accepts from SonicWALL, a nonexclusive, nontransferable (except as otherwise set forth herein) and nonsublicensable license (“License”) to:

(i) execute and use the Software on the Hardware with which the Software is provided (pre-installed) in accordance with the applicable Documentation; and,

(ii) for Software provided in standalone form (without Hardware), install, execute and use the Software on the Hardware or hardware device(s) on which it is intended to be used in accordance with the applicable Documentation and the License purchased. If Customer purchased multiple copies of standalone Software, Customer’s License to such standalone Software includes the right to install, use and execute up to the number of copies of Software Licenses purchased.

In addition, the License includes the right to (x) make a reasonable number of additional copies of the Software to be used solely for non-productive archival purposes, and (y) make and use copies of the end user documentation for Hardware and/or Software provided with the Products (“Documentation”) as reasonably necessary to support Customer’s authorized users in their use of the Products.

(b) License Limitations. Order acknowledgments, Documentation and/or the particular type of the Products/ Licenses purchased by Customer may specify limits on Customer’s use of the Software, and which limits apply to the License(s) granted hereunder for such Software. Such limits may consist of limiting the term of the License, or the number or amount of nodes, storage space, sessions, calls, users, subscribers, clusters, devices, ports, bandwidth, throughput or other elements, and/or require the purchase of separate Licenses to use or obtain particular features, functionalities, services, applications or other items. Use of the Software shall be subject to all such limitations.

(c) For Customer’s Internal Business. Each License shall be used by Customer solely to manage its own internal business operations as well as the business operations of its Affiliates. Notwithstanding the foregoing, if Customer is in the regular business of providing firewall, VPN or Security management for a fee to entities that are not its Affiliates (“MSP Customers”), Customer may use the Products for its MSP Customers provided that either (i) Customer, and not MSP Customers, maintain control and possession of the Products, or (ii) if MSP Customers have possession and/or control of Products in whole or in part, this Agreement must be provided to MSP Customers and they must agree that their use of the Products is subject to the terms and conditions of this Agreement. Customer agrees to indemnify and hold SonicWALL harmless from and against any claims by MSP Customers against SonicWALL relating to the Products and/or Customer’s services for MSP Customers. “Affiliate” means any legal entity controlling, controlled by, or under common control with a party to this Agreement, but only for so long as such control relationship exists.

(d) Evaluation License. If the Software is provided by SonicWALL or a Reseller at no charge for evaluation purposes, then Section 1(a) above shall not apply to such Software and instead Customer is granted a nonproduction License to use such Software and the associated documentation solely for Customer’s own internal evaluation purposes for an evaluation period of up to thirty (30) days from the date of delivery of the Software, plus any extensions granted by SonicWALL in writing (the "Evaluation Period"). There is no fee for Customer’s use of the Software for nonproduction evaluation purposes during the Evaluation Period, however, Customer is responsible for any applicable shipping charges or taxes which may be incurred, and any fees which may be associated with usage beyond the scope permitted herein. Notwithstanding anything otherwise set forth in this Agreement, Customer understands and agrees that evaluation Software is provided “AS IS” and that SonicWALL does not provide a warranty or maintenance services for evaluation Licenses.

(e) Restrictions. Customer may not (i) modify, translate, localize, adapt, rent, lease, loan, create or prepare derivative works of, or create a patent based on the Software or any part thereof, (ii) make copies except as expressly authorized under this Agreement, (iii) copy the Software onto any public or distributed network, (iv) modify or resell the Software, use the Software in connection with the operation of any nuclear facilities, or use for purposes which are competitive to SonicWALL, or (v) except as expressly authorized in Section 2(c) above, operate the Software for use in any time-sharing, outsourcing, service bureau or application service provider type environment. Unless and except to the extent authorized in the applicable Documentation, Software provided with and/or as the Product, in part or whole, is licensed for use only in accordance with the Documentation as part of the Product: Software components making up a Product may not be separated from, nor used on a separate or standalone basis from the Product. Each permitted copy of the Software and Documentation made by Customer hereunder must contain all titles, trademarks, copyrights and restricted rights notices as in the original. Customer understands and agrees that the Products may work in conjunction with third party products and Customer agrees to be responsible for ensuring that it is properly licensed to use such third party products. Any Software provided in object code form is licensed hereunder only in object code form. Except to the extent allowed by applicable law if located in the European Union, and then only with prior written notice to SonicWALL, Customer shall not disassemble or reverse engineer the Software in whole or in part or authorize others to do so. Customer agrees not to use the Software to perform comparisons or other "benchmarking" activities, either alone or in connection with any other software or service, without SonicWALL's written permission; or publish any such performance information or comparisons.

(f) Third Party Software. There may be certain third party owned software provided along with, or incorporated within, the Products ("Third Party Software"). Except as set forth below, such Third Party Software shall be considered Software governed by the terms and conditions of this Agreement. However, some Products may contain other Third Party Software that is provided with a separate license agreement, in which case such Third Party Software will be governed exclusively by such separate license agreement ("Third Party License") and not this Agreement. Any such Third Party Software that is governed by a Third Party License, and not this Agreement, will be identified on the applicable Product page on SonicWALL's website and/ or in a file provided with the Product. Except as SonicWALL may otherwise inform Customer in writing, the Third Party License gives Customer at least the license rights granted above, and may provide additional license rights as to the Third Party Software, but only with respect to the particular Third Party Software to which the Third Party License applies. SUCH THIRD PARTY SOFTWARE UNDER A THIRD PARTY LICENSE IS PROVIDED WITHOUT ANY WARRANTY FROM SONICWALL AND ITS SUPPLIERS, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. Notwithstanding the foregoing, SonicWALL shall honor its warranty, maintenance and support obligations in respect to the SonicWALL Products regardless of whether the warranty, maintenance or support issue is caused in whole or in part by the Third Party Software provided by SonicWALL with the Product.

(g) Updates/Upgrades. If Customer purchases or otherwise is eligible to receive a SOFTWARE update or upgrade, you must be properly licensed to use the Product identified by SonicWALL as being eligible for the update/ upgrade in order to install and use the SOFTWARE update/ upgrade. A SOFTWARE update/ upgrade replaces and/or supplements the Software Product that formed the basis for your eligibility for the update/upgrade, and does not provide you an additional License (copy) of the Software to use separately from the Software Product to be updated/ upgraded. You may use the resulting updated/upgraded Product only in accordance with the terms of this Agreement.

(h) Activation Keys May Expire. Certain Products, including Security Services that provide regular ongoing updates for Software (e.g., Security Service consisting of anti-virus signature updates), may come with an activation key or license key (a key that must be entered to activate the Product, "Activation Key"). If the Activation Key for a Product is not activated within five (5) years from the date of issuance by SonicWALL, such Activation Key(s) may expire and no

longer activate the Product. Products that come with an expiring Activation Key will operate for the contracted term of the License (or purchased Security Service), so long as the Activation Key is activated within five (5) years from SonicWALL's date of issuance.

2. OWNERSHIP

SonicWALL and its licensors are the sole and exclusive owners of the Software, and all underlying intellectual property rights in the Hardware. All rights not expressly granted to Customer are reserved by SonicWALL and its licensors.

3. TERMINATION OF LICENSE(S)

All licenses to the Software hereunder shall terminate if Customer fails to comply with any of the provisions of this Agreement and does not remedy such breach within thirty (30) days after receiving written notice from SonicWALL. Customer agrees upon termination to immediately cease using the Software and to destroy all copies of the Software which may have been provided or created hereunder.

4. SUPPORT SERVICES

SonicWALL's current Support Service offerings ("Support Services") and the terms and conditions applicable to such Support Services are set forth in SonicWALL's Support Services Terms located http://www.sonicwall.com/us/support/ Services.html and are incorporated herein by reference. Support Services may require an additional fee. Unless otherwise agreed to in writing, SonicWALL's Support Services are subject to SonicWALL's Support Services Terms which are in effect at the time the Support Services are purchased by Customer, and these terms and conditions will be incorporated herein by reference at that time. SonicWALL reserves the right to change the Support Services Terms from time to time by posting such changes on its website, which shall apply to any Support Services purchased on or after the date of such posting.

5. SONICWALL WARRANTY

(a) Warranty. SonicWALL warrants to Customer (original purchaser Customer only) that for the applicable warranty period ("Warranty Period") the Hardware will be free from any material defects in materials or workmanship and the Software, if any, will substantially conform to the Documentation applicable to the Software and the License purchased ("Limited Warranty"). Except as may indicated otherwise in writing by SonicWALL, the Warranty Period for Hardware is one year from the date of registration of the Hardware Product (or if sooner, seven days after initial delivery of the Hardware Product to Customer), and the applicable warranty period for Software is ninety days from the date of registration of the Software Product (or if sooner, seven days after initial delivery/download) of the Software Product to/by Customer. SonicWALL does not warrant that use of the Product(s) will be uninterrupted or error free nor that SonicWALL will correct all errors. The Limited Warranty shall not apply to any non-conformance (i) that SonicWALL cannot recreate after exercising commercially reasonable efforts to attempt to do so; (ii) caused by misuse of the Product or by using the Product in a manner that is inconsistent with this Agreement or the Documentation; (iii) arising from the modification of the Products by anyone other than SonicWALL; or (iv) caused by any problem or error in third party software or hardware not provided by SonicWALL with the Product regardless of whether or not the SonicWALL Product is designed to operate with such third party software or hardware. SonicWALL's sole obligation and Customer's sole and exclusive remedy under any express or implied warranties hereunder shall be for SonicWALL to use commercially reasonable efforts to provide error corrections and/or, if applicable, repair or replace parts in accordance with

SonicWALL's Support Services Terms. Customer shall have no rights or remedies under this Limited Warranty unless SonicWALL receives Customer's detailed written warranty claim within the applicable warranty period.

(b) Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH ABOVE, TO MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW SONICWALL HEREBY DISCLAIMS ON BEHALF OF ITSELF, ITS SUPPLIERS, DISTRIBUTORS AND RESELLERS ALL WARRANTIES, EXPRESS, STATUTORY AND IMPLIED, APPLICABLE TO THE PRODUCTS, SERVICES AND/OR THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE.

6. LIMITATION OF LIABILITY

The Products are not designed, manufactured, authorized or warranted to be suitable for use in any system where a failure of such system could result in a situation that threatens the safety of human life, including without limitation any such medical, life support, aviation or nuclear applications. Any such use and subsequent liabilities that may arise from such use are totally the responsibility of Customer, and all liability of SonicWALL, whether in contract, tort (including without limitation negligence) or otherwise in relation to the same is excluded. Customer shall be responsible for mirroring its data, for backing it up frequently and regularly, and for taking all reasonable precautions to prevent data loss or corruption. SonicWALL shall not be responsible for any system downtime, loss or corruption of data or loss of production. NOTWITHSTANDING ANYTHING ELSE IN THIS AGREEMENT OR OTHERWISE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SONICWALL, ITS SUPPLIERS, DISTRIBUTORS OR RESELLERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST OR CORRUPTED DATA, LOST PROFITS OR SAVINGS, LOSS OF BUSINESS OR OTHER ECONOMIC LOSS OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, ARISING OUT OF OR RELATED TO THIS AGREEMENT, THE PRODUCTS OR THE SERVICES, WHETHER OR NOT BASED ON TORT, CONTRACT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND WHETHER OR NOT SONICWALL HAS BEEN ADVISED OR KNEW OF THE POSSIBILITY OF SUCH DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, SONICWALL'S MAXIMUM LIABILITY TO CUSTOMER ARISING FROM OR RELATING TO THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNTS RECEIVED BY SONICWALL FOR THE PRODUCTS AND THE SERVICES PURCHASED BY CUSTOMER, PROVIDED THAT WHERE ANY CLAIM AGAINST SONICWALL RELATES TO PARTICULAR PRODUCT AND/OR SERVICES, SONICWALL'S MAXIMUM LIABILITY SHALL BE LIMITED TO THE AGGREGATE AMOUNT RECIEVED BY SONICWALL IN RESPECT OF THE PRODUCTS AND/OR SERVICES PURCHASED BY CUSTOMER AFFECTED BY THE MATTER GIVING RISE TO THE CLAIM. (FOR MAINTENANCE SERVICES OR A PRODUCT SUBJECT TO RECURRING FEES, THE LIABILITY SHALL NOT EXCEED THE AMOUNT RECEIVED BY SONICWALL FOR SUCH MAINTENANCE SERVICE OR PRODUCT PURCHASED BY CUSTOMER DURING THE TWELVE (12) MONTHS PRECEDING THE CLAIM). CUSTOMER EXPRESSLY AGREES TO THE ALLOCATION OF LIABILITY SET FORTH IN THIS SECTION, AND ACKNOWLEDGES THAT WITHOUT ITS AGREEMENT TO THESE LIMITATIONS, THE PRICES CHARGED FOR THE PRODUCTS AND SERVICES WOULD BE HIGHER.

7. GOVERNMENT RESTRICTIONS

Customer agrees that it will not export or re-export the Products without SonicWALL's prior written consent, and then only in compliance with all requirements of applicable law, including but not limited to U.S. export control regulations. Customer has the responsibility to obtain any required licenses to export, reexport or import the Products. Customer shall defend, indemnify and hold SonicWALL and its suppliers harmless from any claims arising out of Customer's

violation of any export control laws relating to any exporting of the Products. By accepting this Agreement and receiving the Products, Customer confirms that it and its employees and agents who may access the Products are not listed on any governmental export exclusion lists and will not export or re-export the Products to any country embargoed by the U.S. or to any specially denied national (SDN) or denied entity identified by the U.S. Applicable export restrictions and exclusions are available at the official web site of the U.S. Department of Commerce Bureau of Industry and Security (www.bis.doc.gov). For purchase by U.S. governmental entities, the technical data and computer software in the Products are commercial technical data and commercial computer software as subject to FAR Sections 12.211, 12.212, 27.405-3 and DFARS Section 227.7202. The rights to use the Products and the underlying commercial technical date and computer software is limited to those rights customarily provided to the public purchasers as set forth in this Agreement. The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

8. GENERAL

a) Governing Law and Venue. This Agreement shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflict of laws principles that would require the application of laws of a different state. The parties agree that neither the United Nations Convention on Contracts for the International Sale of Goods, nor the Uniform Computer Information Transaction Act (UCITA) shall apply to this Agreement, regardless of the states in which the parties do business or are incorporated. Any action seeking enforcement of this Agreement or any provision hereof shall be brought exclusively in the state or federal courts located in the County of Santa Clara, State of California, United States of America. Each party hereby agrees to submit to the jurisdiction of such courts. Notwithstanding the foregoing, SonicWALL is entitled to seek immediate injunctive relief in any jurisdiction in the event of any alleged breach of Section 1 and/or to otherwise protect its intellectual property.

b) Assignment. Except as otherwise set forth herein, Customer shall not, in whole or part, assign or transfer any part of this Agreement or any rights hereunder without the prior written consent of SonicWALL. Any attempted transfer or assignment by Customer that is not permitted by this Agreement shall be null and void. Any transfer/assignment of a License that is permitted hereunder shall require the assignment/transfer of all copies of the applicable Software along with a copy of this Agreement, the assignee must agree to all terms and conditions of this Agreement as a condition of the assignment/transfer, and the License(s) held by the transferor Customer shall terminate upon any such transfer/assignment.

c) Severability. If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, such provision will be enforced to the maximum extent permissible and the remaining provisions of this Agreement will remain in full force and effect.

d) Privacy Policy. Customer hereby acknowledges and agrees that SonicWALL’s performance of this Agreement may require SonicWALL to process or store personal data of Customer, its employees and Affiliates, and to transmit such data within SonicWALL or to SonicWALL Affiliates, partners and/or agents. Such processing, storage, and transmission may be used for the purpose of enabling SonicWALL to perform its obligations under this Agreement, and as described in SonicWALL’s Privacy Policy (www.SonicWALL.com/us/Privacy_Policy.html, “Privacy Policy”) and may take place in any of the countries in which SonicWALL and its

Affiliates conduct business, including countries outside of the European Economic Area. SonicWALL reserves the right to change the Privacy Policy from time to time as described in the Privacy Policy.

e) Notices. All notices provided hereunder shall be in writing, delivered personally, or sent by internationally recognized express courier service (e.g., Federal Express), addressed to the legal department of the respective party or to such other address as may be specified in writing by either of the parties to the other in accordance with this Section.

f) Disclosure of Customer Status. SonicWALL may include Customer in its listing of customers and, upon written consent by Customer, announce Customer's selection of SonicWALL in its marketing communications.

g) Waiver. Performance of any obligation required by a party hereunder may be waived only by a written waiver signed by an authorized representative of the other party, which waiver shall be effective only with respect to the specific obligation described therein. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

h) Force Majeure. Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control, and without its fault or negligence, including without limitation, acts of God, strikes, lockouts, riots, acts of war, epidemics, communication line failures, and power failures.

i) Audit. Customer shall maintain accurate records to verify compliance with this Agreement. Upon request by SonicWALL, Customer shall furnish (a copy of) such records to SonicWALL and certify its compliance with this Agreement.

j) Headings. Headings in this Agreement are for convenience only and do not affect the meaning or interpretation of this Agreement. This Agreement will not be construed either in favor of or against one party or the other, but rather in accordance with its fair meaning. When the term “including” is used in this Agreement it will be construed in each case to mean “including, but not limited to.”

k) Entire Agreement. This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter hereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any judicial proceeding that may involve the Agreement. This Agreement represents the complete agreement and understanding of the parties with respect to the subject matter herein. This Agreement may be modified only through a written instrument signed by both parties.